PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-307496

(43)Date of publication of application : 19.11.1993

---

(51)Int.Cl. G06F 11/30

G06F 11/30

G06F 13/00

H04L 9/06

H04L 9/14

---

(21)Application number : 04-110599 (71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

N T T FUANETSUTO SYST KK

(22)Date of filing : 30.04.1992 (72)Inventor : WADA YASUSHI

OKUBO TSUNEO

TAZAWA SATOSHI

YOSHIZAWA MASAHIRO

HAYASHI MASAHIRO

---

(54) REMOTE MAINTENANCE DEVICE AND MAINTAINING METHOD

(57)Abstract:

PURPOSE: To improve the safety of communication by storing common key information or key information decoding information as the contents of all key information storage devices.

CONSTITUTION: After starting, a processing request (command) which a working system control part 1-1 can execute is transmitted from a maintenance system control part 4-1 to the working system control part 1-1. This command is encoded in an encoder 2-2 by employing the information of the key information

storage device 5, and is sent to a line 10. At that time, even if the encoded information is intercepted at some place on the line 10 by a malicious third person, the information can not be decoded within a practical period of time as far as he has no information of the key information storage device 5. Besides, even if the same malicious third person transmits the command for obstruction to the working system control part 1-1 from the line 10 in order to obstruct the processing of the working system control part 1-1, as far as he does not know the information of the key information storage device 5, a decoder 3-1 never reproduces it into a significant command.

LEGAL STATUS [Date of request for examination] 04.03.1999

[Date of sending the examiner's decision of rejection] 29.02.2000

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] In the control maintenance system by which the maintenance equipment for maintaining this digital-information-processing equipment through a communication line is connected to one thru/or two or more digital-information-processing equipments The equipment which accumulates key information into all digital-information-processing equipments and the above-mentioned maintenance equipment, Control maintenance equipment

characterized by forming the encoder which encodes a signal with reference to this key information, and the decryption machine which decrypts the encoded signal, and accumulating common key information thru/or key information decode information as contents of the key information storage equipment of all above.

[Claim 2] When maintenance equipment is connected to the location distant from the installation of digital-information-processing equipment through a communication line and an inconvenient condition generates this maintenance equipment to this digital-information-processing equipment, In the maintenance procedure which restores an inconvenient condition immediate -- log information -- using -- the above -- The control maintenance approach characterized by enciphering from this digital-information-processing equipment and this maintenance equipment using the encoder and decryption machine in which the signal sent out to the above-mentioned communication line was formed by these all digital-information-processing equipments, and the key information storage equipment used for coding/decryption.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to the equipment which maintains the equipment which processes the digital information of a computer, a digital controller, a digital exchange, etc. from a remote place, and its maintenance procedure.

[0002]

[Description of the Prior Art] Conventionally, in respect of mass-production nature, high-performance-izing, and a raise in reliance, the equipment which processes digital information has a remarkable advance, and has spread in the large field. Especially the failure rate per element components improves remarkably by integration (LSI-izing) of components. Consequently, the big thing of the scale of integration components also becomes possible, and digital-information-processing equipment came to be used in various fields. By the way, it will be divided into the in bed type built into the interior of a (b) system, and the (b) external world and an opening type with a digital interface if digital-information-processing equipment is classified. Since the scale of an in bed type is small and it generally bears a part of function of a system, informational I/O is indirect and its amount of information to treat is also relatively small. On the other hand, an opening type has a large scale, it is the

independent system in many cases, and the amount of information to deal with is [informational I/O is direct and] relatively large. Next, if "maintenance" is defined, it can be defined as changing the function of digital-information-processing equipment into 'the condition that it can be used immediately'. That is, it is fixing and restoring this, when ** digital-information-processing equipment's loses a function or is in the condition (that is, failed state) the engine performance's not being satisfied, and when information is already held, new information cannot be accepted or ** digital-information-processing equipment cannot continue processing, it is evacuation (backup) of the information, and performing deletion and changing into the condition which can be processed. Moreover, as a definition of a wide sense, the thing of an action which avoids that it foresees resulting in the 'inconvenient condition' of having been stated to the above-mentioned ****, and will pre-be in the condition is said for a while.

[0003] When digital-information-processing equipment was an in bed type, while the system use person (operator) containing it operated it, the failed state was detected, and it exchanged the whole components, or it detected that the amount of information storage reached the limitation, operated carrying out the depression of the reset button for canceling information etc., and the operator was performing substantial maintenance on that spot according to the operating

manual. On the other hand, since the equipment scale is generally large when digital-information-processing equipment is an opening type, when the equipment is in 'an inconvenient condition', an operator may be unable to distinguish whether it is in the failed state of the aforementioned **, and whether it is in the condition of the processing continuation impossible of the aforementioned **. Then, the maintainer by the side of an equipment vendor goes to the installation of equipment, and performs distinction and repair of being 'an inconvenient condition'. Thus, an equipment scale enlarges that a maintainer goes out and it is in the inclination which a function follows on complicating and increases. However, since the number of maintainers is limited, satisfying maintenance is difficult. Moreover, in order to cause increase of the charge of maintenance for a user, it also becomes hesitating at installation of digital-information-processing equipment. However, on the actual problem that a maintainer is insufficient, there is conflict that the ratio of the transit time by a means of transportation until it goes to an equipment installation etc. is larger than the time amount to which a maintainer is engaged in actual maintenance business.

[0004]

[Problem(s) to be Solved by the Invention] Then, next, in order to lessen transit time, the approach of installing a recovery system in a remote place was used.

For example D. L.Burkes & R.KTreiber "DesignApproaches for Real-Time Transaction Processing Remote Site Recovery and Dig. Pap.COMPCON Spring Since it enables it to correspond immediately as stated to pp.568-572 and 1990" even if 'inconvenient conditions' are any of the aforementioned ** and **, The recovery system was installed in the remote place other than the working system in the installation of equipment, and duplication distribution of a database was realized. Consequently, when un-arranging other than a certain hardware failure occurred to a working system, it enabled it to restore a working system immediately from a recovery system using log information (processing record). Moreover, it enables it to restore a working system in the shortest period, after fixing it also in the case of the failure of hardware. However, since the installation of a recovery system is in a remote place, much important information will be delivered and received through a network. Consequently, in a network, the software called the 'virus' destroyed with malice mixes the program and data of the digital-information-processing equipment connected to it, or a possibility that it may be monitored outside also has information. That is, there is risk of a safe communication link being threatened. The purpose of this invention can solve such a conventional technical problem, can make meaningless to persons other than the user of normal making meaningless work of the virus mixed via a (b) network, and information monitored through a (b) network, and is to offer the

control maintenance equipment and the maintenance procedure which can perform the high communication link of safety.

[0005]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, the control maintenance equipment of this invention In the control maintenance system by which the maintenance equipment for maintaining digital-information-processing equipment through a communication line is connected to one (b) thru/or two or more digital-information-processing equipments The equipment which accumulates key information into all digital-information-processing equipments and maintenance equipment, The encoder which encodes a signal with reference to key information, and the decryption machine which decrypts the encoded signal are formed, and the description is to accumulate common key information thru/or key information decode information as contents of all the key information storage equipments. Moreover, when the control maintenance approach of this invention connects maintenance equipment to the location distant from the installation of (b) digital-information-processing equipment through a communication line and an inconvenient condition generates maintenance equipment to digital-information-processing equipment, In the maintenance procedure which restores an inconvenient condition immediate -- log information -- using -- the

above -- The description is to encipher from digital-information-processing equipment and maintenance equipment using the encoder and decryption machine in which the signal sent out to a communication line was formed by all the digital-information-processing equipments, and the key information storage equipment used for coding/decryption.

[0006]

[Function] In this invention, the information spread on a network in order to make meaningless work of the virus mixed via a network is enciphered, and in order to make meaningless in addition to the user of normal making detection possible at the time of a decryption of the code, and the information itself monitored through a network, a holder in bad faith makes it decode difficulty. Therefore, key information storage equipment, an encoder, and a decryption machine are formed in all 1 thru/or two or more digital-information-processing equipments which interconnects through the communication line, and maintenance equipment. Since the signal sent out to a communication line is enciphered through an encoder and a decryption machine from all information processors and maintenance equipment, even if it becomes impossible for a third person to monitor information through a communication line and he makes a virus mix, since a decryption machine discards this, no bad influence is received.

[0007]

[Example] Hereafter, a drawing explains the example of this invention to a detail. Drawing 1 is the block diagram of a working system and a maintenance system showing the 1st example of this invention. The working system 1 is installed in the equipment installation 8, and the working database 6 and an encoder 2-1, the decryption machine 3-1, and key information storage equipment 5 are connected to the working system control section 1-1 in a working system. Moreover, there is a maintenance-system installation 9 in the working system installation 8 and the distant location 9, and the maintenance system 4 is installed there. RIKABARIDE-Thabet-SU 7 and an encoder 2-2, the decryption machine 3-2, and key information storage equipment 5 are connected to the maintenance-system control section 4-1. When the data memorized by the working database 6 are lost by RIKABARIDE-Thabet-SU 7, the same data are memorized to the duplex so that it can recover immediately. Usually, the working system control section 1-1 is interlocked with the working database 6, and is performing original processing in the working system installation 8. The maintainer who stays at the working system installation 8 and the left maintenance-system installation 9 starts the maintenance-system control section 4-1, and does the line connection between an encoder 2-1 and the decryption machines 3-2 and of between an encoder 2-2 and the decryption machines 3-1 using the digital service unit which is not illustrated, respectively.

May use two different circuits with directivity, and it does not have directivity, i.e., the approach of this line connection may be performed using one circuit in which two-way communication is possible.

[0008] After starting, the processing demand (command) which can perform the working system control section 1-1 is transmitted from the maintenance-system control section 4-1 to the working system control section 1-1. In an encoder 2-2, it encodes using the information on key information storage equipment 5, and this command is sent out to a circuit 10. In this case, the technique encoded, i.e., an algorithm, is realizable by choosing the technique suitable for employment about coding/decryption rate and dependability of a code as indicated by for example, **** Kazuo, Nakamura **** "cipher system and application" information processing Vol.32, No.6, and pp.714-723. Even when the encoded information is monitored by the holder in bad faith at one point of the circuits 10, unless it has the information on key information storage equipment 5, information is undecipherable in practical time amount. Moreover, since a decoder 3-1 is not reproduced to a significant command unless the information on key information storage equipment 5 is known even if the same holder in bad faith is the purpose which blocks processing of the working system control section 1-1 and transmits the command for active jamming from a circuit 10 to the working system control section 1-1, the working system control section 1-1 can leave the command for

active jamming. In addition, like [in the case of accumulating the information on the working database 6 in RIKABARIDE-Thabet-SU 7], when a communication link is sent out from the working system control section 1-1 to the maintenance-system control section 4-1, an encoder 2-1 is used instead of an encoder 2-2, and the decryption machine 3-2 is used instead of the decryption machine 3-1, respectively.

[0009] Drawing 2 is the operation flow chart of drawing 1 . Sequence of operation is performed in general in order of step 1 to the step 20. First, the digital service unit of the maintenance-system control section 4-1 chooses the digital service unit of the working system control section 1-1 (step 1), establishes a circuit mutually (step 2), and completes a line connection mutually. Next, the maintenance maintenance-system control section 4-1 transmits a command to execute in the working system control section 1-1 (step 3). And a command is enciphered and it is sent out to a circuit (steps 4 and 5). So far, (steps 1-5), a maintenance system 4 is performed with a subject. Next, reception of the enciphered command and the decryption to the command of an ordinary format are performed (steps 6 and 7). Next, the working system 1 receives a command and performs processing corresponding to it (step 8). When the information which should be transmitted to a maintenance system 4 exists in the contents of processing, information is packet-ized, and the packet which enciphered it is

repeated, and it transmits/receives, decrypts again, and a maintenance system 4 stores or displays the information (steps 9-14). The working system 1 serves as a subject, the processing (steps 6-11) so far is performed, and, as for steps 12-14, a maintenance system 4 is performed with a subject.

[0010] If processing is completed, after the working system's 1 creating a response message in a packet format and enciphering it, it transmits to a circuit (steps 15-17). And a maintenance system 4 receives the enciphered packet, decrypts it, and displays it on a display etc. (steps 18 and 19). If there is a command which should be processed continuously at the end, it will return to step 3 and processing will be continued (step 20). In drawing 2 , immediately after steps 5, 11, and 17, since the packet which had the circuit top enciphered flows, even if a holder in bad faith monitors information, the information cannot be restored. Moreover, just behind steps 5, 11, and 17, since it is decrypted with a key 5 at steps 7, 13, and 19, respectively even if it pours in malignant packet information, such as a virus, it is not restored to the packet format (packet format before encryption) of the normal used for this system system, and is recognized as an abnormality packet, and after registering with a log file, it is rejected.

[0011] Drawing 3 is the block diagram of a working system and a maintenance system showing the 2nd example of this invention. In drawing 3 , there are two or more working system installations 8, and the working system 1 is installed in

each. Even if it adjoins, it may be separated from the working system installation 8. With these working system installations, the maintenance-system installation 9 is in the distant location, and the maintenance system 4 is installed in it. Two or more working systems 1 and one maintenance system 4 are connected to the circuit 10. The circuit 10 has the bus structure, is the point which does not have a bad influence on signal propagation in near the system installations 8 and 9, and can connect it to systems 1 and 4. In such a configuration, two or more working systems 1 and one maintenance system 4 contain key information storage equipment 5 inside, respectively, and the contents are also communalized. Thereby, a maintenance system 4 can perform maintenance to the working system 1 of arbitration.

[0012] Drawing 4 is the block diagram of a working system and a maintenance system showing the 3rd example of this invention. The same notation as drawing 1 and drawing 3 expresses the same thing. In drawing 4 , it is prepared as a different thing from them instead of a public key 11 and a public key 12 being keys 5. A public key 11 is a public key for decoding the coding information of a maintenance system 4, and a public key 12 is a public key for decoding the coding information of the working system 1. The public key cryptosystem is indicated by the Oyama work "development (1) mathematical principle [of a code], and latest" Institute of Electronics, Information and Communication

Engineers, Vol.73, No.5, and pp.513-525, for example. Since the decryption key of the working system 1 cannot be known even if a holder in bad faith monitors in case the information on a public key (coding key) 12 is delivered from the working system 1 to a maintenance system 4 so that clearly from this reference, there is an advantage that the coding information itself is undecipherable. Code delivery can be carried out on-line by using a public key 12 similarly.

[0013]

[Effect of the Invention] Since it can repulse easily according to this invention even if it minds a communication line, and it monitors communication link information and a holder in bad faith makes malignant information, such as a virus, mix on a communication line as explained above, it is possible to perform the high communication link of safety.

[0014]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is the block diagram of a working system and a maintenance system showing the 1st example of this invention.

[Drawing 2] It is an operation flow chart in drawing 1 .

[Drawing 3] It is the block diagram of a working system and a maintenance system showing the 2nd example of this invention.

[Drawing 4] It is the block diagram of a working system and a maintenance system showing the 3rd example of this invention.

[Description of Notations]

1 Working System

4 Maintenance System

8 Working System Installation

9 Maintenance-System Installation

1-1 Working System Control Section

2-1, 2-2 Encoder

3-1, 3-2 Decryption machine

4-1 Maintenance-System Control Section

5 Key Information Storage Equipment

6 Working Database

7 RIKABARIDE-Thabet-SU

11 12 Public key are recording equipment

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－307496

(43)公開日　平成５年(1993)11月19日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　11/30	Ｄ	9290－5Ｂ		
	３２０　Ｇ	9290－5Ｂ		
13/00	３５１　Ｚ	7368－5Ｂ		
Ｈ０４Ｌ　9/06				
		7117－5Ｋ	Ｈ０４Ｌ　9/ 02　Ｚ	

審査請求　未請求　請求項の数２(全　７　頁)　最終頁に続く

(21)出願番号　特願平4－110599

(22)出願日　平成４年(1992)４月30日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号

(71)出願人　592095332
エヌ・ティ・ティ・ファネット・システムズ株式会社
東京都大田区久が原２丁目23番18号

(72)発明者　和田　康
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　磯村　雅俊

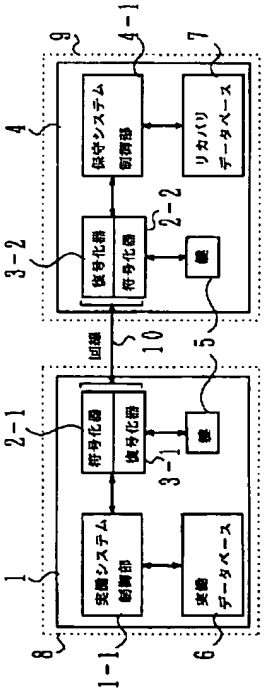
最終頁に続く

(54)【発明の名称】　遠隔保守装置および保守方法

(57)【要約】

【目的】　実働システムと保守システムとが遠隔回線を介して接続されている場合に、悪意の第三者がウィルスを混入しても、また通信回線を介して傍受しようとしても、正規の利用者以外の者には意味のないものにして、それらの行為を無駄に終らせる。

【構成】　実働システムと保守システムの両方に、鍵情報蓄積装置と符号化器と復号化器を備えて、蓄積された鍵を参照することにより、伝送する全ての情報を符号化して回線に送出し、受信した全ての情報を復号化する。これにより、通信の安全化を図る。



1

【特許請求の範囲】

【請求項1】　1つないし複数のディジタル情報処理装置に、通信回線を介して該ディジタル情報処理装置を保守するための保守装置が接続されている遠隔保守システムにおいて、全てのディジタル情報処理装置および上記保守装置内に、鍵情報を蓄積する装置と、該鍵情報を参照して信号を符号化する符号化器と、符号化された信号を復号化する復号化器とを設け、上記全ての鍵情報蓄積装置の内容として、共通の鍵情報ないし鍵情報解読情報を蓄積することを特徴とする遠隔保守装置。

【請求項2】　ディジタル情報処理装置の設置場所から離れた場所に通信回線を介して保守装置を接続し、該保守装置は該ディジタル情報処理装置に不都合な状態が発生したとき、即座にログ情報を利用して上記不都合な状態を修復する保守方法において、該ディジタル情報処理装置および該保守装置から上記通信回線に送出する信号を、該ディジタル情報処理装置の全てに設けられた符号化器および復号化器と、符号化／復号化に使用する鍵情報蓄積装置を使用して暗号化することを特徴とする遠隔保守方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、コンピュータ、ディジタル制御装置、およびディジタル交換機等のディジタル情報を処理する装置を遠隔地から保守する装置ならびにその保守方法に関する。

【０００２】

【従来の技術】従来より、ディジタル情報を処理する装置は量産性、高性能化、高信頼化の点で進歩が目覚ましく、広い分野で普及されている。特に、要素部品当りの故障率は、部品の集積化（ＬＳＩ化）により著しく改善されている。その結果、集積化部品の規模が大きなものも可能となり、種々の分野でディジタル情報処理装置が利用されるようになった。ところで、ディジタル情報処理装置を分類すると、（イ）システムの内部に組み込まれているインベッドタイプと、（ロ）外界とディジタルインタフェースを持つオープンタイプとに分けられる。インベッドタイプは、一般にその規模が小さく、システムの機能の一部を担うために情報の入出力は間接的であり、扱う情報量も相対的に小さい。他方、オープンタイプは規模が大きく、独立したシステムであることが多く、情報の入出力は直接的で、取り扱う情報量は相対的に大きい。次に、『保守』の定義を行うと、ディジタル情報処理装置の機能を‘直ちに使用できる状態’にすること、と定義することができる。すなわち、①ディジタル情報処理装置が機能を失ったり、性能を満足できない状態（つまり、故障状態）にあるときには、これを修理・修復することであり、また②ディジタル情報処理装置が既に情報を保持して、新たな情報を受け入れたり、処理を継続することができないときには、その情報の退避

2

（バックアップ）や、抹消を行い、処理可能な状態にすることである。また、少し広義の定義としては、上記①②に述べられた‘不都合な状態’に到ることを予見して、予めその状態になることを回避する行為のことを言う。

【０００３】ディジタル情報処理装置がインベッドタイプの場合には、それを含むシステムの使用者（オペレータ）が操作中に故障状態を検出して、部品ごと取り替えたり、情報蓄積量が限界に達したことを検出して、情報を破棄するためのリセットボタンを押下する等の操作を行って、オペレータが操作マニュアルに従ってその場で実質的な保守を行っていた。一方、ディジタル情報処理装置がオープンタイプの場合には、一般に装置規模が大きいので、その装置が‘不都合な状態’にある場合に、オペレータは前記①の故障状態にあるのか、前記②の処理継続不能の状態にあるのか、判別できないことがある。そこで、装置ベンダ側の保守担当者が装置の設置場所に出向いて、‘不都合な状態’か否かの判別や修理を行うことにしている。このように、保守担当者が出向くのは、装置規模が大型化して、機能が複雑化するに伴って増加する傾向にある。しかしながら、保守担当者の数は限定されているため、満足のいく保守は困難である。また、ユーザにとっては保守料の増額を招くため、ディジタル情報処理装置の導入をためらうことにもなる。ただし、保守担当者不足の実際の問題では、保守担当者が実際の保守業務に携わる時間よりも、装置設置場所に出向くまでの交通機関等による移動時間の比率の方が大きいというような矛盾もある。

【０００４】

【発明が解決しようとする課題】そこで、次に、移動時間を少なくするために、遠隔地にリカバリシステムを設置する方法を用いた。例えば、D. L. Burkes & R. K. Treiber『Design Approaches for Real-Time Transaction Processing Remote Site Recovery, Dig. Pap. COMPCON, Spring, pp.568～572, 1990』に述べられているように、‘不都合な状態’が前記①, ②のいずれであっても、即時に対応できるようにするため、装置の設置場所にある実働システムの他に遠隔地にリカバリシステムを設置して、データベースの重複分散を実現した。その結果、実働システムに何らかのハードウェア障害以外の不都合が発生した場合、ログ情報（処理記録）を利用してリカバリシステムから即座に実働システムを修復することができるようにした。また、ハードウェアの障害の場合にも、それを修理後に最短期間で実働システムを修復することができるようにしている。しかしながら、リカバリシステムの設置場所が遠隔地にあるため、多数の重要な情報がネットワークを介して授受されることになる。その結果、ネットワークでは、それに接続されているディジタル情報処理装置のプログラムやデータを悪意をもって破壊する‘ウィル

ス’と呼ばれるソフトウェアが混入したり、情報が外部に傍受されるおそれもある。すなわち、安全な通信が脅かされる危険がある。本発明の目的は、このような従来の課題を解決し、（イ）ネットワーク経由で混入するウィルスの働きを無意味にすること、および（ロ）ネットワークを介して傍受される情報を正規の利用者以外の者に無意味にすることができ、安全性の高い通信を行える遠隔保守装置および保守方法を提供することにある。

【０００５】

【課題を解決するための手段】上記目的を達成するため、本発明の遠隔保守装置は、（イ）１つないし複数のディジタル情報処理装置に、通信回線を介してディジタル情報処理装置を保守するための保守装置が接続されている遠隔保守システムにおいて、全てのディジタル情報処理装置および保守装置内に、鍵情報を蓄積する装置と、鍵情報を参照して信号を符号化する符号化器と、符号化された信号を復号化する復号化器とを設け、全ての鍵情報蓄積装置の内容として、共通の鍵情報ないし鍵情報解読情報を蓄積することに特徴がある。また、本発明の遠隔保守方法は、（ロ）ディジタル情報処理装置の設置場所から離れた場所に通信回線を介して保守装置を接続し、保守装置はディジタル情報処理装置に不都合な状態が発生したとき、即座にログ情報を利用して上記不都合な状態を修復する保守方法において、ディジタル情報処理装置および保守装置から通信回線に送出する信号を、ディジタル情報処理装置の全てに設けられた符号化器および復号化器と、符号化／復号化に使用する鍵情報蓄積装置を使用して暗号化することに特徴がある。

【０００６】

【作用】本発明においては、ネットワーク経由で混入するウィルスの働きを無意味にするために、ネットワーク上に伝搬する情報を暗号化して、その暗号の復号化時に検出可能にすること、およびネットワークを介して傍受される情報自体を正規の利用者以外には無意味にするために、悪意の第三者が解読困難にする。そのために、通信回線を介して相互接続されている１ないし複数のディジタル情報処理装置と保守装置の全てに、鍵情報蓄積装置と符号化器と復号化器とを設ける。全ての情報処理装置および保守装置から通信回線に送出する信号は、符号化器および復号化器を通して暗号化されるので、第三者は通信回線を介して情報を傍受することができなくなり、またウィルスを混入させても、復号化器がこれを廃棄するので、何の悪影響も受けることがない。

【０００７】

【実施例】以下、本発明の実施例を、図面により詳細に説明する。図１は、本発明の第１の実施例を示す実働システムと保守システムのブロック図である。装置設置場所８には実働システム１が設置され、実働システム内の実働システム制御部１－１には実働データベース６および符号化器２－１、復号化器３－１、および鍵情報蓄積装置５が接続されている。また、実働システム設置場所８と離れた場所９には、保守システム設置場所９があり、そこに保守システム４が設置されている。保守システム制御部４－１には、リカバリデータベース７および符号化器２－２、復号化器３－２、および鍵情報蓄積装置５が接続されている。リカバリデータベース７には、実働データベース６に記憶されたデータが失われた場合に、即座に回復できるように、二重に同一データを記憶しておく。通常は、実働システム制御部１－１は実働データベース６と連動して、実働システム設置場所８において本来の処理を実行している。実働システム設置場所８と離れた保守システム設置場所９に滞在する保守担当者は保守システム制御部４－１を起動し、図示されない回線接続装置を用いて符号化器２－１と復号化器３－２の間、および符号化器２－２と復号化器３－１の間をそれぞれ回線接続する。この回線接続の方法は、方向性を持つ２つの異なる回線を用いてもよく、また方向性を持たない、つまり双方向通信が可能な１つの回線を用いて行ってもよい。

【０００８】起動した後に、保守システム制御部４－１から実働システム制御部１－１に対して、実働システム制御部１－１が実行可能な処理要求（コマンド）を送信する。このコマンドは、符号化器２－２において、鍵情報蓄積装置５の情報を利用して符号化され、回線１０に送出される。この場合に符号化される手法、つまりアルゴリズムは、例えば、宝木和夫、中村勤著『暗号方式と応用』情報処理Ｖol.32,No.6,pp.714～723に記載されているように、暗号の符号化/復号化速度や信頼性について、運用に適した手法を選択することにより実現できる。符号化された情報が回線１０のいずれかの地点で悪意の第三者により傍受された場合でも、鍵情報蓄積装置５の情報を持たない限り、実用的な時間内に情報を解読できない。また、同じ悪意の第三者が、実働システム制御部１－１の処理を妨害する目的で、回線１０から妨害用コマンドを実働システム制御部１－１に対して送信しても、鍵情報蓄積装置５の情報を知らない限り、復号器３－１は有意なコマンドに再生しないので、実働システム制御部１－１は妨害用コマンドを捨て去ることが可能である。なお、実働データベース６の情報をリカバリデータベース７に蓄積する場合のように、通信が実働システム制御部１－１から保守システム制御部４－１に対して送出されるときには、符号化器２－２の代りに符号化器２－１が、復号化器３－１の代りに復号化器３－２が、それぞれ使用される。

【０００９】図２は、図１の動作フローチャートである。動作順序は、概ねステップ１からステップ２０の順に行われる。先ず、保守システム制御部４－１の回線接続装置が実働システム制御部１－１の回線接続装置を選択し（ステップ１）、相互間に回線を確立して（ステップ２）、相互間に回線接続を完了する。次に、保守保守

システム制御部４－１が実働システム制御部１－１で実行したいコマンドを送信する（ステップ３）。そして、コマンドが暗号化され、回線に送出される（ステップ４，５）。ここまでは（ステップ１～５）、保守システム４が主体で実行される。次に、暗号化されたコマンドの受信と、通常形式のコマンドへの復号化が行われる（ステップ６，７）。次に、実働システム１がコマンドを受信し、それに対応する処理を実行する（ステップ８）。もし、処理内容に保守システム４に送信すべき情報が存在する場合には、情報をパケット化して、それを暗号化したパケットを繰り返し送信／受信して、再度復号化して保守システム４がその情報を格納したり、表示したりする（ステップ９～１４）。ここまでの処理（ステップ６～１１）は、実働システム１が主体となって実行され、ステップ１２～１４は、保守システム４が主体で実行される。

【００１０】処理が終了したならば、実働システム１は、応答メッセージをパケット形式で作成して、それを暗号化した後、回線に送信する（ステップ１５～１７）。そして、保守システム４は、暗号化したパケットを受信し、それを復号化して、ディスプレイ等に表示する（ステップ１８，１９）。最後に、継続して処理すべきコマンドがあれば、ステップ３に戻って処理を継続する（ステップ２０）。図２において、ステップ５，１１，１７の直後は、回線上を暗号化されたパケットが流れるので、悪意の第三者が情報を傍受しても、その情報を復元できない。また、ステップ５，１１，１７の直後で、ウィルス等の悪性のパケット情報を注入しても、ステップ７，１３，１９でそれぞれ鍵５により復号化されるので、このシステム体系で使用される正規のパケット形式（暗号化前のパケット形式）に復元されることはなく、異常パケットと認識されて、ログファイルに登録後に棄却される。

【００１１】図３は、本発明の第２の実施例を示す実働システムと保守システムのブロック図である。図３においては、複数の実働システム設置場所８があり、実働システム１がそれぞれに設置されている。実働システム設置場所８は、隣接していても、また離れていてもよい。これらの実働システム設置場所とは離れた場所に、保守システム設置場所９があり、保守システム４が設置されている。複数の実働システム１と１つの保守システム４は回線１０に接続されている。回線１０は、バス構造を有しており、システム設置場所８，９の近傍のうち信号伝搬に悪影響を及ぼさない地点で、システム１，４に接続することができる。このような構成において、複数の実働システム１と１つの保守システム４は、内部にそれぞれ鍵情報蓄積装置５を含んでおり、かつその内容も共

通化されている。これにより、保守システム４は任意の実働システム１に対して保守を行うことが可能である。

【００１２】図４は、本発明の第３の実施例を示す実働システムと保守システムの構成図である。図１，図３と同一の記号は、同一のものを表わしている。図４では、それらと異なるものとして、公開鍵１１および公開鍵１２が鍵５の代りに設けられている。公開鍵１１は、保守システム４の暗号情報を解読するための公開鍵であり、公開鍵１２は、実働システム１の暗号情報を解読するための公開鍵である。公開鍵暗号方式については、例えば、小山著『暗号の数理と最近の発展（１）』電子情報通信学会誌、Vol.73,No.5,pp.513～525に記載されている。この文献からも明らかなように、実働システム１から公開鍵（符号化鍵）１２の情報を保守システム４に配送する際に、悪意の第三者が傍受しても、実働システム１の復号化鍵を知ることができないので、暗号情報自体を解読することはできないという利点がある。公開鍵１２も、同じように用いることにより、暗号配送をオンラインで実施できる。

【００１３】

【発明の効果】以上説明したように、本発明によれば、悪意の第三者が通信回線を介して通信情報を傍受したり、またウィルス等の悪性の情報を通信回線上に混入させたりしても、簡単に撃退することができるので、安全性の高い通信を行うことが可能である。

【００１４】

【図面の簡単な説明】

【図１】本発明の第１の実施例を示す実働システムと保守システムのブロック図である。

【図２】図１における動作フローチャートである。

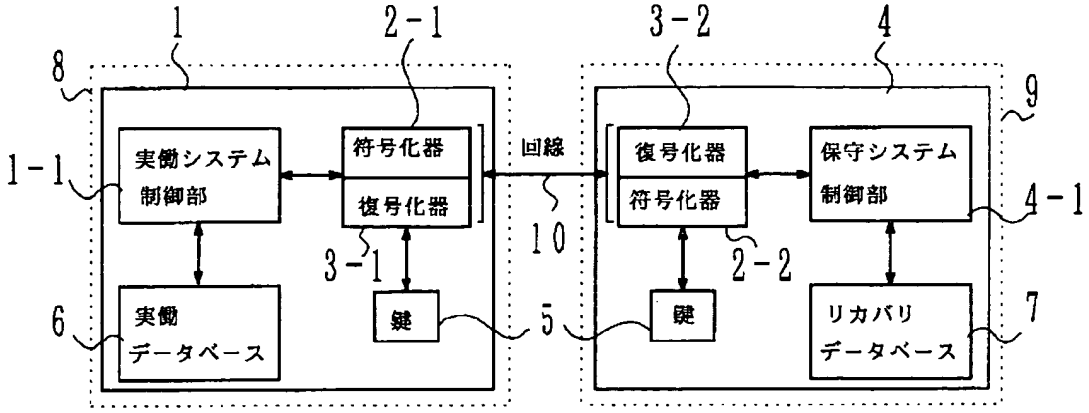
【図３】本発明の第２の実施例を示す実働システムと保守システムのブロック図である。

【図４】本発明の第３の実施例を示す実働システムと保守システムのブロック図である。

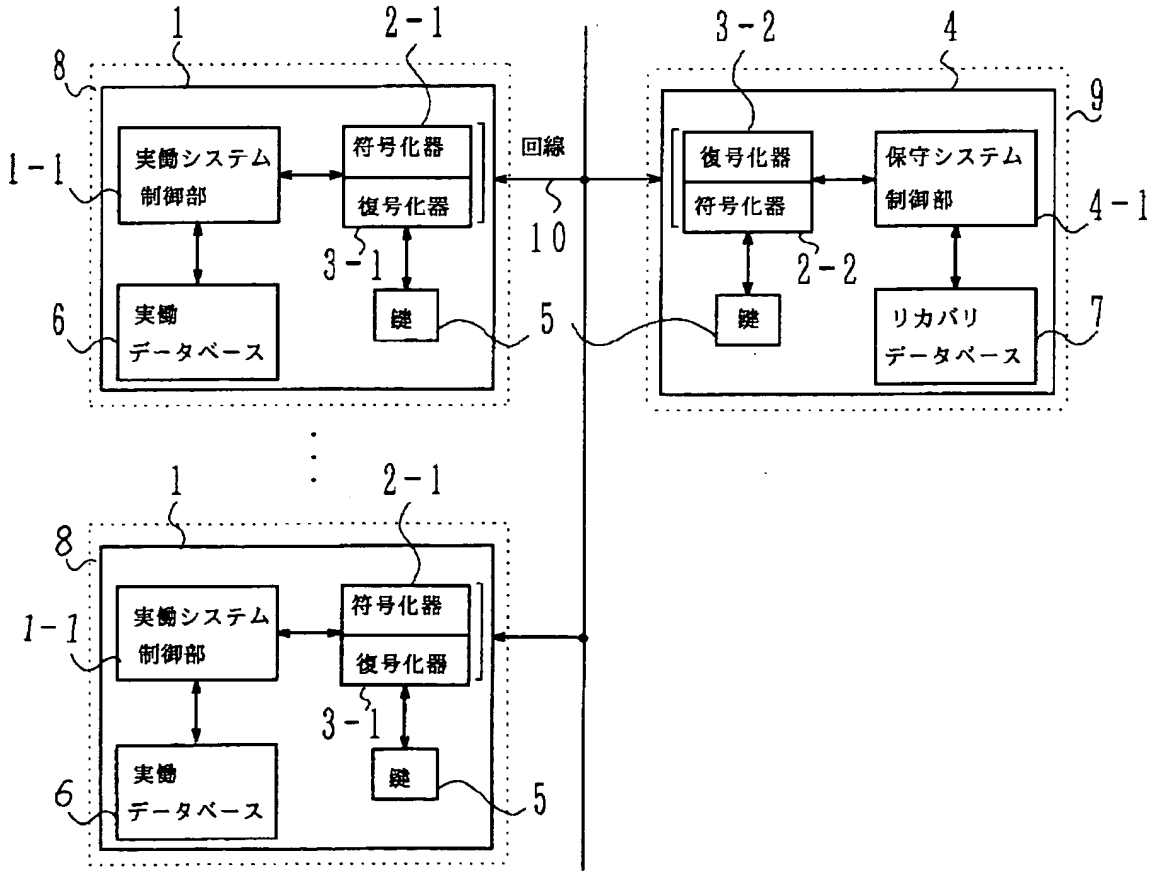
【符号の説明】

１　実働システム
４　保守システム
８　実働システム設置場所
９　保守システム設置場所
１－１　実働システム制御部
２－１，２－２　符号化器
３－１，３－２　復号化器
４－１　保守システム制御部
５　鍵情報蓄積装置
６　実働データベース
７　リカバリデータベース
１１，１２　公開鍵蓄積装置

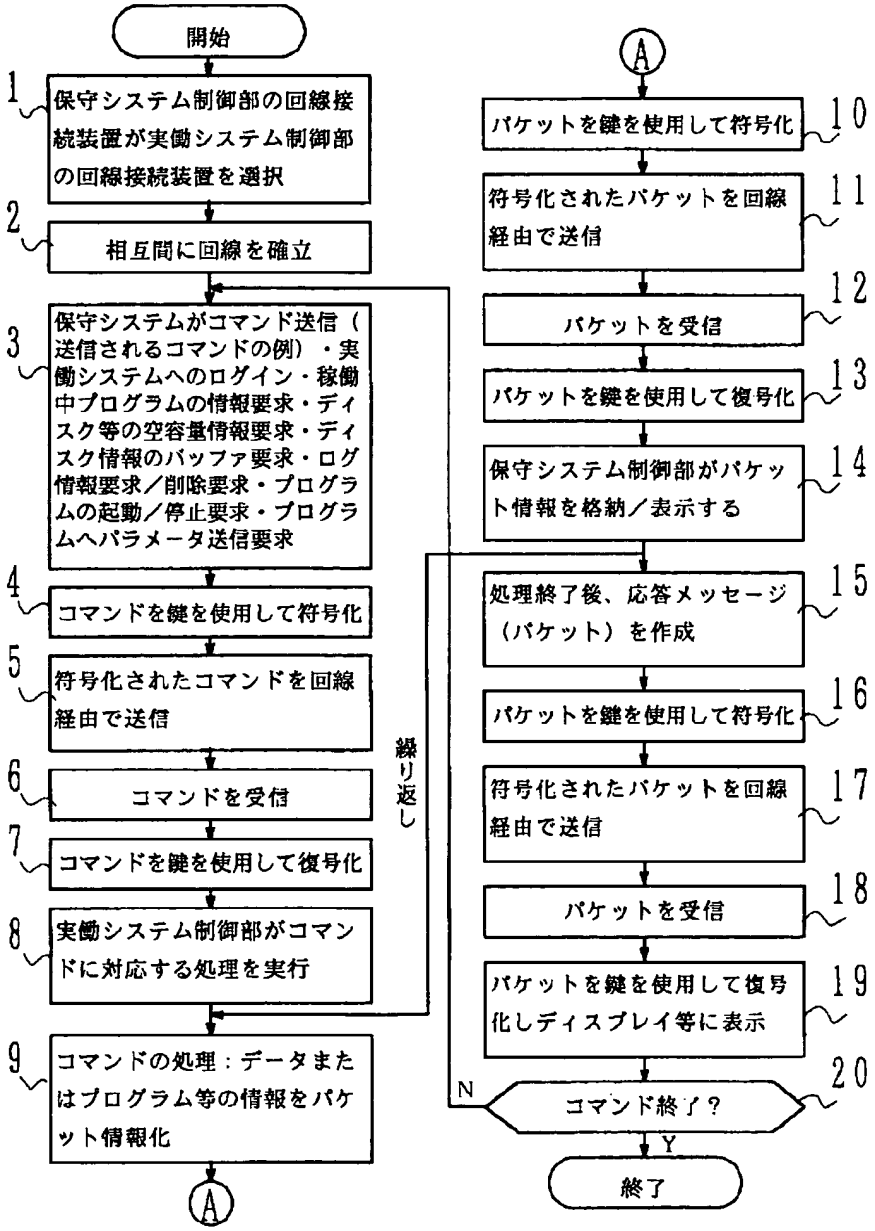
【図１】


1
2-1
3-2
4
8
9
1-1
実働システム
制御部
符号化器
復号化器
回線
10
復号化器
符号化器
保守システム
制御部
4-1
3-1
2-2
6
実働
データベース
鍵
5
鍵
リカバリ
データベース
7

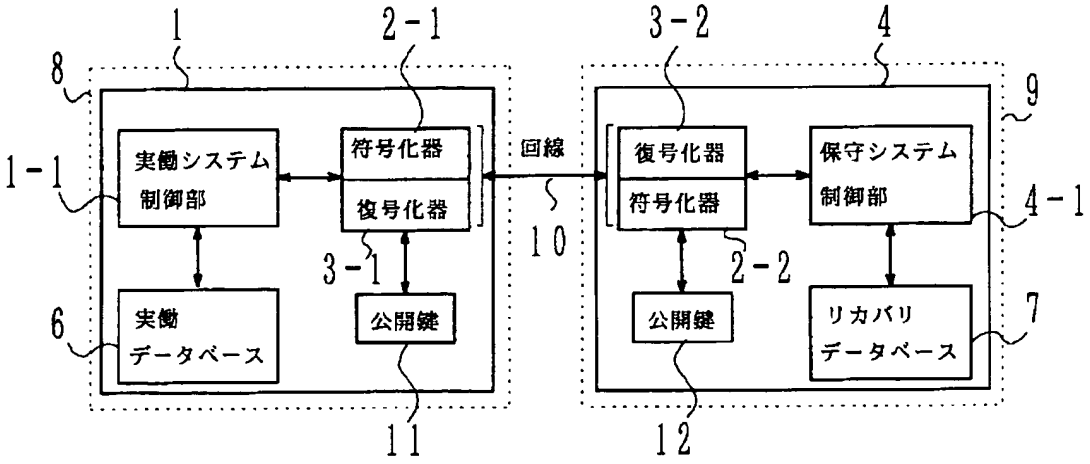
【図３】


1
2-1
3-2
4
8
9
1-1
実働システム
制御部
符号化器
復号化器
回線
10
復号化器
符号化器
保守システム
制御部
4-1
3-1
2-2
6
実働
データベース
鍵
5
鍵
リカバリ
データベース
7
1
2-1
8
1-1
実働システム
制御部
符号化器
復号化器
3-1
6
実働
データベース
鍵
5

【図2】


開始
1
保守システム制御部の回線接続装置が実働システム制御部の回線接続装置を選択
2
相互間に回線を確立
3
保守システムがコマンド送信（送信されるコマンドの例）・実働システムへのログイン・稼働中プログラムの情報要求・ディスク等の空容量情報要求・ディスク情報のバッファ要求・ログ情報要求／削除要求・プログラムの起動／停止要求・プログラムへパラメータ送信要求
4
コマンドを鍵を使用して符号化
5
符号化されたコマンドを回線経由で送信
6
コマンドを受信
7
コマンドを鍵を使用して復号化
8
実働システム制御部がコマンドに対応する処理を実行
9
コマンドの処理：データまたはプログラム等の情報をパケット情報化
A
繰り返し
A
10
パケットを鍵を使用して符号化
11
符号化されたパケットを回線経由で送信
12
パケットを受信
13
パケットを鍵を使用して復号化
14
保守システム制御部がパケット情報を格納／表示する
15
処理終了後、応答メッセージ（パケット）を作成
16
パケットを鍵を使用して符号化
17
符号化されたパケットを回線経由で送信
18
パケットを受信
19
パケットを鍵を使用して復号化しディスプレイ等に表示
20
コマンド終了？
N
Y
終了

【図４】



フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/14				

(72)発明者　大久保　恒夫
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　田沢　聰
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　吉沢　正浩
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内
(72)発明者　林　正博
東京都中央区日本橋堀留町１丁目５番７号　エヌ・ティ・ティ・ファネット・システムズ株式会社内